ĐẠI HỌC QUỐC GIA THÀNH PHỐ HỒ CHÍ MINH
TRƯỜNG ĐẠI HỌC KHOA HỌC TỰ NHIÊN
KHOA CÔNG NGHỆ THÔNG TIN
----oOo----

BÁO CÁO ĐỒ ÁN

|Giáo viên hướng dẫn|

Lương Vĩ Minh
Phạm Thị Bạch Huệ
Tiết Gia Hồng

Học phần: An toàn và bảo mật dữ liệu trong hệ thống thông tin

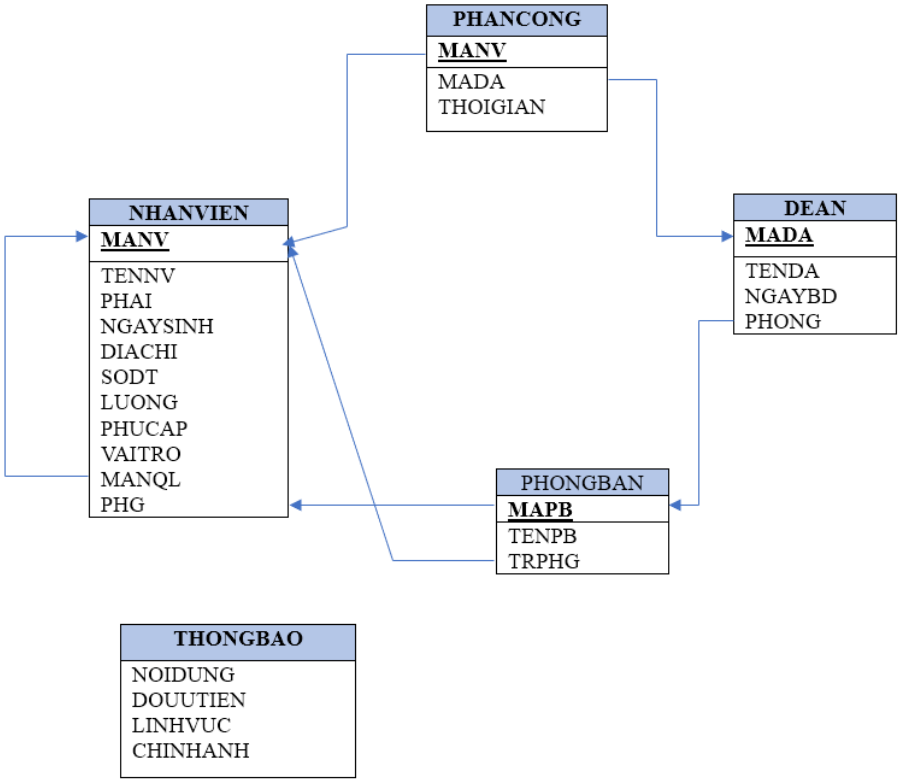
Thành phố Hồ Chí Minh, tháng 06 năm 2023

Mục lục

1. Bảng phân công và đánh giá thành viên:

MSSV	Họ tên	Phân công	Hoàn thành
20120056	Trần Quốc Đỉnh	Viết báo cáo, làm chính sách, OLS, Audit	100%
20120060	Nguyễn Trí Đức	Viết báo cáo, làm giao diện và mã hóa	100%
20120169	Hoàng Đình Ngọc Quang	Làm chính sách, OLS, Audit và back end	100%
20120248	Nguyễn Thế Anh	Làm giao diện, mã hóa và cơ sở dữ liệu	100%

2. Lược đồ CSDL:



Hình 2.1 Lược đồ CSDL

*Bảng THONGBAO dành riêng cho OLS.

3. Phân tích đồ án:

Nhóm đồ án sẽ phân tích 6 tiêu chí ban đầu thông qua các Chính sách bảo mật: DAC, RBAC, VPD, OLS, giám sát hành động trên dữ liệu bằng Audit, bảo vệ các thông tin nhạy cảm bằng Encrypt.

3.1 Tóm tắt loại người dùng trong hệ thống và vai trò của họ

Hệ thống quản lý thông tin nhân viên và việc tham gia đề án của nhân viên bao gồm 6 vai trò(Role) là: Nhân viên, Quản lý trực tiếp, Trưởng phòng, Tài chính, Nhân sự, Trưởng đề án, Ban giám đốc.

Database có một user admin là OLS_TEST1, sử dụng PDB là XEPDB1.

Tóm tắt các chính sách:

	NHANVIEN	PHANCONG	PHONGBAN	DEAN
Nhân viên	R_{myself} $U_{myself(ns,dc,sdt)}$	R_{myself}	R_{all}	R_{all}
Quản lý trực tiếp	R_{myself} ,$R_{myemployee}$ $U_{myself(ns,dc,sdt)}$	R_{myself} $R_{myemployee}$	R_{all}	R_{all}
Trưởng phòng	$R_{mydepartment}$ $U_{myself(ns,dc,sdt)}$	$R_{mydepartment}$ $I,U,D_{mydepartment}$	R_{all}	R_{all}
Tài chính	R_{all} $U_{all(luong,phucap)}$	R_{all}	R_{all}	R_{all}
Nhân sự	R_{all} $I,U_{\text{all trừ luong,phucap}}$	R_{myself}	R_{all} I, U_{all}	R_{all}
Trưởng đề án	R_{myself} $U_{myself(ns,dc,sdt)}$	R_{myself}	R_{all}	R_{all} I, U_{all}
Ban giám đốc	R_{all} $U_{myself(ns,dc,sdt)}$	R_{all}	R_{all}	R_{all}

3.2Chính sách bảo mật mật DAC và RBAC:

3.2.1 Tóm lược lý thuyết:

Oracle hỗ trợ quản lý người dùng bằng role, user, và grant privilege.

- Một user là người dùng hệ thống, có username và password để đăng nhập vào cơ sở dữ liệu.
- Một quyền (privilege) là 1 sự cho phép thực hiện 1 câu lệnh SQL nào đó hoặc được phép truy xuất đến một đối tượng nào đó.
- Role là một tập hợp bao gồm các quyền và các role khác. Role được gán cho các user hoặc các role khác. Role giúp cho việc quản trị người dùng dễ dàng và tiết kiệm công sức hơn.

Ngoài ra các câu lệnh như GRANT, REVOKE,… để quản lý quyền hạn của một user hay một role khi đăng nhập vào database.

3.2.2 Đề xuất kịch bản cài đặt

Tương ứng với các người dùng, sẽ có 6 ROLE:

- Nhân viên(NhanVien): 250 users.
- Quản lý trực tiếp(QuanLyTrucTiep): 20 users.
- Trưởng phòng(TruongPhong): 8 users.
- Tài chính(TaiChinh): 5 users.
- Nhân sự(NhanSu): 5 users.
- Trưởng đề án(TruongDeAn): 3 users.
- Ban giám đốc(BanGiamDoc): 5 users.

Sau đó Grant Role tương ứng với các user. Và các user sẽ có cú pháp Tên đăng nhập là: “NV”+MANV ; mật khẩu chung: 123

	NHANVIEN	PHANCONG	DEAN	PHONGBAN
NHANVIEN	R, $U_{(ns,dc,sdt)}$	R	R	R
QLTRUCTIEP	R, $U_{(ns,dc,sdt)}$	R	R	R

TRUONGPHONG	R, $U_{(ns,dc,sdt)}$	R, I, U, D	R	R
TAICHINH	R, $U_{(ns,dc,sdt,lg,pc)}$	R	R	R
NHANSU	R, I, $U_{(all\ trừ\ lg,\ pc)}$	R	R	R, I, U
TRUONGDEAN	R, $U_{(ns,dc,sdt)}$	R	R,I,U,D	R
BANGIAMDOC	R, $U_{(ns,dc,sdt)}$	R	R	R

3.3 Chính sách bảo mật VPD:

3.3.1 Tóm lược lý thuyết:

- VPD cho phép giới hạn việc truy xuất các hàng (row) dựa trên một chính sách bảo mật (security policy).
- Để thực hiện VPD, đầu tiên ta tạo 1 hàm PL/SQL (PL/SQL function) trả về một chuỗi (string). Chuỗi này chứa các điều kiện của chính sách bảo mật mà ta muốn hiện thực. Hàm PL/SQL vừa được tạo ở trên sau đó được đăng ký cho các table, view mà ta muốn bảo vệ bằng cách dùng package PL/SQL DBMS_RLS.
- Khi có một câu truy vấn của bất kỳ user nào trên đối tượng được bảo vệ, Oracle sẽ nối chuỗi được trả về từ hàm nêu trên vào mệnh đề WHERE của câu lệnh SQL ban đầu (nếu trong câu lệnh SQL ban đầu không có mệnh đề WHERE thì Oracle sẽ tự động tạo thêm mệnh đề WHERE để đưa chuỗi điều kiện vào), nhờ đó sẽ lọc được các hàng dữ liệu theo các điều kiện của chính sách bảo mật. Nhiều chính sách bảo mật khi thêm vào một bảng thì Oracle sẽ gộp các điều kiện theo phép AND.

3.1.2 Đề xuất kịch bản cài đặt:

Vì chỉ có Quản lý nhân viên và Trưởng phòng là phải cấp quyền kiểm soát mức độ điều kiện trên dòng nên ta sẽ lựa chọn việc cài VPD cho 2 vai trò này. Thực hiện cài đặt VPD cho 2 vai trò trên cả 2 bảng NHANVIEN và PHANCONG.

- Khởi tạo một function return ra vai trò (role) của tài khoản nhân viên trong hệ thống.
- Khởi tạo VPD điều kiện đáp ứng yêu cầu trên view của bảng NHANVIEN đã được tạo ra và được cấp quyền select trên view này cho 2 vai trò.
- Khởi tạo VPD đáp ứng yêu cầu trên bảng PHANCONG cho cả 2 vai trò.

3.4 Chính sách bảo mật OLS:

3.4.1 Tóm lược lý thuyết:

- Để sử dụng được OLS trước hết chúng ta phải đăng ký và kích hoạt tính năng OLS, mặc định Oracle không có tính năng OLS. Sau đó kích hoạt user LBACSYS.
- Data label (Nhãn dữ liệu): gồm 3 loại thành phần là level, compartment, group. Nếu một Table (bảng) có chính sách OLS thì mỗi hàng dữ liệu sẽ được gán một data label.
    - Về level, khi khai báo level, ta sẽ gán cho nó một "dạng số" (oracle cho phép từ 0 đến 9999). Dạng số có giá trị (level) càng cao sẽ có độ nhạy cảm càng cao.
    - Về compartment, OLS cho phép tối đa 10000 compartments trong một chính sách. Compartment giúp cho việc phân loại dữ liệu, ví dụ như theo lĩnh vực, chuyên ngành, dự án,…chứ không thể hiện sự phân cấp mức độ nhạy cảm của dữ liệu đó.
    - Về group, OLS cho phép tối đa 10000 groups trong một chính sách. Group giúp thể hiện cơ cấu kế thừa ví dụ như những tổ chức, cơ quan, bộ phận nào sở hữu hoặc quản lý dữ liệu,… Do vậy group có cấu trúc cây phân cấp. Một group có thể thuộc một group cha và có nhiều group con. Dữ liệu thuộc một group con thì được xem như cũng thuộc group cha.

- Cú pháp của một data label (Có thể được Oracle tự động gán hoặc người dùng tự gán một label tag):

3.4.2 Kịch bản cài đặt:

Cài đặt OLS trên pluggable database đã chọn, cài đặt môi trường để sử dụng OLS.

Khởi tạo bảng THONGBAO với các cột NOIDUNG, DOUUTIEN, LINHVUC, CHINHANH ứng với nhãn của yêu cầu.

Thực hiện OLS trên bảng THONGBAO và gắn nhãn cho từng dòng trong bảng.

Cuối cùng là gắn nhãn đúng theo yêu cầu cho các tài khoản người dùng trong hệ thống.

3.5 Chính sách bảo mật Audit:

3.5.1 Tóm lược lý thuyết:

- Auditing là hoạt động giám sát và ghi lại dựa trên các hoạt động cá nhân như thực hiện câu lệnh SQL, hay dựa trên sự kết hợp các yếu tố bao gồm tên, ứng dụng, thời gian,… Các chính sách bảo mật có thể dẫn đến việc audit khi những thành phần tử cụ thể trong CSDL Oracle bị truy cập hay thay thế.
- Auditing được sử dụng:
- Các kiểu giám sát (types of auditing):
    - Cho phép giải trình những hành động hiện tại tham gia vào một schema, table, dòng riêng biệt, hay một nội dung cụ thể nào đó.
    - Ngăn cản user khỏi hành động không thích hợp dựa trên trách nhiệm phải giải trình đó.
    - Điều tra các hoạt động đáng ngờ. Ví dụ, nếu một user không được phép đang xoá dữ liệu từ một bảng nào đó thì người quản trị bảo mật sẽ ghi lại tất cả những kết nối CSDL và tất cả những hành động xoá các dòng từ bảng trong CSDL dù thành công hay không thành công.
    - Thông báo cho người giám sát rằng có user bất hợp pháp đang thao tác hay xoá dữ liệu hay user có nhiều quyền hệ thống hơn sự cho phép.

    - Giám sát và thu thập dữ liệu về các hoạt động CSDL cụ thể. Ví dụ, người quản trị CSDL có thể thu thập thống kê về thông tin các bảng đang được update, hay bao nhiêu users cùng truy cập vào thời điểm cực đỉnh.
- Các kiểu giám sát (types of auditing):
    - Oracle cho phép giám sát theo 2 lựa chọn tập trung hoặc mở rộng.
        - Sự thực thi câu lệnh thành công, hoặc không thành công, hoặc cả 2 Mỗi lần thực thi câu lệnh trong mỗi session của user, hay bất kì khi nào mà câu lệnh được thực thi
        - Hoạt động của tất cả các user hay của một user cụ thể nào đó.
    - Có 4 kiểu giám sát:
        - Statement auditing: chia thành 2 nhóm
            - Câu lệnh DDL: Ví dụ AUDIT TABLE giám sát tất cả các câu lệnh CREATE và DROP TABLE.
            - Câu lệnh DML: Ví dụ AUDIT SELECT TABLE giám sát tất cả câu lệnh SELECT trên bảng và view.
        - Privilege auditing: Kiểm tra việc sử dụng quyền hệ thống, ví dụ AUDIT CREATE TABLE. Privilege auditing được chú trọng hơn statement auditing vì nó chỉ kiểm tra việc sử dụng một số quyền nhất định. Có thể đặt privilege auditing giám sát những user được lựa chọn hay giám sát mọi user.
        - Schema object auditing: Kiểm tra câu lệnh cụ thể trên đối tượng schema cụ thể, ví dụ AUDIT SELECT ON NHANVIEN. (Rất được chú trọng). Schema object auditing luôn áp dụng cho tất cả các user.
        - Fine-grained auditing: Kiểm tra dữ liệu truy xuất và các hoạt động dựa trên nội dung của dữ liệu đó. Ví dụ: Sử dụng DBMS_FGA, người quản trị bảo mật tạo ra một chính sách kiểm tra trên một bảng. Nếu bất kì dòng nào trả về từ câu lệnh DML thoả điều kiện kiểm tra thì một mục về sự kiện kiểm tra sẽ được chèn vào trong audit trail.
- Kích hoạt Standard Audit Trail:
    - Bất cứ database user hợp pháp nào cũng có thể thiết lập lựa chọn giám sát đối với câu lệnh, quyền và đối tượng bất cứ khi nào. Tuy nhiên CSDL Oracle không sinh thông tin audit cho Standard database audit

trail trừ khi CSDL giám sát được kích hoạt. Người quản trị bảo mật thường có trách nhiệm điều khiển việc giám sát này.

- Chức năng Audit mặc định bị bất hoạt, nhưng có thể kích hoạt nó bằng cách thiết lập giá trị cho tham số AUDIT_TRAIL AUDIT_TRAIL = { none | os | db | db,extended | xml | xml,extended }

Để kích hoạt chức năng giám sát, SQL> ALTER SYSTEM SET audit_trail=db SCOPE=SPFILE.

- Bất hoạt lựa chọn Standard Auditing:
  - Câu lệnh NOAUDIT để tắt các lựa chọn giám sát của Oracle.
  - Mệnh đề WHENEVER để tắt các giám sát đối với các câu lệnh được thực hiện thành công hay không thành công. Nếu không sử dụng mệnh đề đó thì chức năng giám sát sẽ tắt cả đối với trường hợp thành công hay thất bại.
  - Mệnh đề BY SESSION/BY ACCESS không được hỗ trợ trong câu lệnh NOAUDIT.
- Chính sách trong Fine-grained Auditing:
  - Chính sách FGA có thể theo dõi việc truy xuất dữ liệu dựa trên nội dung của dữ liệu đó. Sử dụng chính sách, ta có thể chỉ rõ cột nào và điều kiện khi nào ta mới cần phải ghi lại việc truy xuất đó. Ta cũng có thể cung cấp thêm tên hàm mà ta muốn thực thi khi một sự kiện giám sát xảy ra. Hàm đó có thể nhắc nhở hoặc báo động cho người quản trị hay xử lí lỗi và các bất thường.

3.5.2 Kịch bản cài đặt:

- Cài đặt Audit trên oracle.
- Cấp quyền execute on dbms_fga cho admin để admin có thể cài đặt fine-grained auditing trên hệ thống.
- Thực hiện cài đặt chính sách auditing trên hệ thống.

3.6 Chính sách mã hóa:

3.6.1 Tóm lược lý thuyết:

- Mã hoá (Encryption) là một quá trình mã hoá dữ liệu. Chuyển dữ liệu gốc (có thể hiểu được) sang bảng mã (không thể hiểu được) để ngụy trang chúng, chỉ

người dùng có thể giải mã mới có thể xem được thông tin trên dữ liệu. Do đó, thông tin được bảo vệ khỏi những người không mong muốn.

- Trong việc quản lý an toàn bảo mật cho cơ sở dữ liệu, việc mã hoá các thông tin nhạy cảm rất quan trọng.
- Mã hoá bao gồm hai thành phần chính sau:
    - Phương pháp mã hóa: AES, DES, RSA…
    - Key dùng để mã hóa (khóa công khai, khóa riêng tư, khóa chung)
- Với vai trò là một người quản trị cơ sở dữ liệu, chúng ta cần chắc chắn rằng các dữ liệu nhạy cảm cần được mã hoá và an toàn trước các tình huống các phương tiện lưu trữ dữ liệu bị đánh cắp hay kẻ xấu muốn tấn công thông qua hệ điều hành, bỏ qua các rào cản của điều khiển truy cập.
- Trong đồ án này chúng em sử dụng phương thức mã hóa bất đối xứng RSA.

Về mã hóa RSA trong đồ án

- Mã hóa RSA là mã hóa bất đối xứng dựa trên bài toán khó phân tích thừa số nguyên tố, hiện là thuật toán mã hóa có mức an toàn cao và được sử dụng rất phổ biến.
- Do độ bảo mật cao và được hỗ trợ rất tốt bởi thư viện ngôn ngữ lập trình C# nên trong đồ án này nhóm sử dụng để thực hiện cơ chế mã hóa cho dữ liệu nhạy cảm.
- Một ưu điểm thấy rõ của việc mã hóa ở mức ứng dụng đó là dữ liệu trong quá trình truyền tin từ Client-Server và Server-Client sẽ được mã hóa. Có nghĩa là dữ liệu nhạy cảm sẽ được nhập và **mã hóa** ở ứng dụng, sau đó gửi cho server. Nếu không có bước mã hóa ở ứng dụng, khi truyền dữ liệu từ Client→Server sẽ là dữ liệu thô gây nguy hiểm nếu bị "nghe lén".

3.6.2 Kịch bản cài đặt:

- User có vai trò là "Tài chính" sẽ thực hiện mã hóa.
- Thay đổi kiểu dữ liệu cột LUONG, PHUCAP thành RAW để lưu dữ liệu đã mã hóa.
- Quản lý khóa:

    + Thiết lập khóa: khóa sẽ được tạo khi "Tài chính" nhập dữ liệu cho LUONG và PHUCAP.

    + Lưu trữ khóa: toàn bộ khóa sẽ được lưu tại ứng dụng dưới dạng file xml.

    + Phục hồi khóa: Việc người dùng quên khóa là không thể xảy ra do file lưu keys được lưu ở ứng dụng và được xử lý tự động trong app.

+ Thay khóa đồng loạt: do khóa được lưu ở trên ứng dụng nên việc thay khóa đồng loạt sẽ làm mất sự thống nhất giữa các client.

4. Demo:

https://github.com/thenguyenltv/ATBM

5. Tài liệu tham khảo:

Tài liệu Oracle:

- https://docs.oracle.com/en/database/oracle/oracle-database/19/dbseg/using-oracle-vpd-to-control-data-access.html#GUID-06022729-9210-4895-BF04-6177713C65A7
- https://docs.oracle.com/en/database/oracle/oracle-database/19/olsag/getting-started-with-oracle-label-security.html#GUID-D0F9D58B-2C35-413F-A8B6-A5C93641819F
- https://docs.oracle.com/database/121/TDPSG/GUID-61259237-5514-4531-AFB4-CF716F93F1E5.htm#TDPSG94440
- https://docs.oracle.com/cd/B19306_01/appdev.102/b14258/d_crypto.htm#BJFGFDFG

Tài liệu thực hành:

- https://studenthcmusedu-my.sharepoint.com/personal/tghong_mso_hcmus_edu_vn/_layouts/15/stream.aspx?id=%2Fpersonal%2Ftghong%5Fmso%5Fhcmus%5Fedu%5Fvn%2FDocuments%2FRecordings%2FATBMHTTT%20%2D%20CQ2020%5F1%20%2D%20LINK%20H%E1%BB%8CC%20L%C3%9D%20THUY%E1%BA%BET%2027%5F3%5F2023%2D20230326%5F082340%2DMeeting%20Recording%2Emp4&ga=1
- https://drive.google.com/drive/folders/1Bvziga-VRr-q2q73sGk8x1_630uVYd-p

Tài liệu khác:

- https://cuuduongthancong.com/pvf/538308/an-toan-va-bao-mat-he-thong-thong-tin//lab-06_virtual-private-database-(1).pdf?src=afile&action=hover
- https://cuuduongthancong.com/pvf/1142844/an-toan-va-bao-mat-he-thong-thong-tin//lab-08_oracle-label-security-(1).pdf?src=afile&action=hover